

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;">SECRET</div> b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;">SECRET</div>			
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>			
<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER <div style="text-align: center; border: 1px solid black; padding: 2px;">PR# - FD2020-04-60670</div>			<input checked="" type="checkbox"/>	a. ORIGINAL <i>(Complete date in all cases)</i> <div style="text-align: center; border: 1px solid black; padding: 2px;">20040329</div>		DATE (YYYYMMDD)
	b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>		REVISION NO.
	c. SOLICITATION OR OTHER NUMBER				c. FINAL <i>(Complete Item 5 in all cases)</i>		DATE (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.							
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>							
a. NAME, ADDRESS, AND ZIP CODE				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
8. ACTUAL PERFORMANCE							
a. LOCATION				b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT AQUISITION, DEVELOPMENT AND CONTRACTOR LOGISTIC SUPPORT FOR THE A-10 TRAINING SYSTEM							
10. CONTRACTOR WILL REQUIRE ACCESS TO:				11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:			
YES NO				YES NO			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION				a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY			
<input checked="" type="checkbox"/> <input type="checkbox"/>				<input type="checkbox"/> <input checked="" type="checkbox"/>			
b. RESTRICTED DATA				b. RECEIVE CLASSIFIED DOCUMENTS ONLY			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input type="checkbox"/> <input checked="" type="checkbox"/>			
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION				c. RECEIVE AND GENERATE CLASSIFIED MATERIAL			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
d. FORMERLY RESTRICTED DATA				d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
e. INTELLIGENCE INFORMATION				e. PERFORM SERVICES ONLY			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input type="checkbox"/> <input checked="" type="checkbox"/>			
(1) Sensitive Compartmented Information (SCI)				f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
(2) Non-SCI				g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input type="checkbox"/> <input checked="" type="checkbox"/>			
f. SPECIAL ACCESS INFORMATION				h. REQUIRE A COMSEC ACCOUNT			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
g. NATO INFORMATION				i. HAVE TEMPEST REQUIREMENTS			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
h. FOREIGN GOVERNMENT INFORMATION				j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS			
<input checked="" type="checkbox"/> <input type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
i. LIMITED DISSEMINATION INFORMATION				k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input type="checkbox"/> <input checked="" type="checkbox"/>			
j. FOR OFFICIAL USE ONLY INFORMATION				l. OTHER <i>(Specify)</i>			
<input checked="" type="checkbox"/> <input type="checkbox"/>				<input checked="" type="checkbox"/> <input type="checkbox"/>			
k. OTHER <i>(Specify)</i>				SEE CONTINUATION SHEET			
<input type="checkbox"/> <input checked="" type="checkbox"/>				<input type="checkbox"/> <input type="checkbox"/>			

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (*Specify*)

OO-ALC/PA
7981 GEORGIA STREET
HILL AFB, UT 84056-5824

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

Compliance with DOD 5220.22M, National Industrial Security Program Operation Manual (NISPOM) for safeguarding classified information to include chapter 8 security requirements for Automated Information Systems. Classification of trainers and AIS is Secret when power is applied or not applied.

SEE CONTINUATION SHEET

13a. Program Official

CURTIS BITTON
OO-ALC/YWB

13b. Duty Phone

801-777-7466
DSN 777-7466

13c. Biennial Review Date

29 MAR 2006

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(*If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

LONG TERM VISITOR GROUP SECURITY AGREEMENT will be executed between the Installation Commander and the Contractor.
See Continuation Sheet

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

See Continuation Sheet

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL
RUDY ROWE

b. TITLE
CONTRACTING OFFICER

c. TELEPHONE (*Include Area Code*)
(801) 775-2099

d. ADDRESS (*Include Zip Code*)
OO-ALC/YWK
6050 GUM LANE, BLDG. 1215
HILL AFB, UT 84056

e. SIGNATURE

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
- ☒ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☒ e. ADMINISTRATIVE CONTRACTING OFFICER
- ☒ f. OTHERS AS NECESSARY

A. Reference Block 1:

Contractor personnel assigned to this program must be U.S. citizens with a minimum of a Secret Security Clearance based on current investigation. Contractor personnel will control access and protect classified information in accordance with the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22M. Contractor personnel must possess the required clearance prior to arrival on-site.

B. Reference Block 8a:

The work effort will be directed from TBD Company, and cage code 1DG67. In addition to the home office, contractor performance will also be conducted at the following sites: Davis Monthan AFB, AZ, Pope AFB, SC, Barksdale AFB, LA, New Orleans JRB, LA, Bradley ANGB, CT, Battle Creek ANGB, MI, Boise ANGB, ID, Whiteman AFB, MO, Osan AB, Korea, Spangdahlem AB, Germany, and the TSSC. The contractor is not authorized to transmit classified information to or from overseas locations.

C. Reference Block 8c:

The cognizant security office is the Chief of Security Forces at the actual location of contractor performance. Reference Blocks 8a and 17 for complete addresses.

D. Reference Block 10a:

COMSEC material /information may not be released to DoD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractors must forward requests for COMSEC material/information to the COMSEC officer through the program office. The contractor is governed by the DoD 5220.22s COMSEC supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances.

E. Reference Block 10a:

The Long Term Visitor Group Agreement between the Installation Commander and Contractor governs access to COMSEC material/information.

F. Reference Block 10g:

Any access to NATO classified information will require a final U.S. Government clearance at the appropriate level, and a NATO briefing.

G. Reference Block 10j:

FOUO information provided shall be safeguarded as specified in the attachment "Protecting for Official Use Only (FOUO) Information".

H. Reference Block 11c:

The contractor will require access to classified source data up to and including Secret in support of this effort. Any extracts or use of such data requires contractor to apply derivative classifications and markings consistent with the source documents. Use of "Multiple Sources" on the "Classified by" line necessitates compliance with the NISPOM, and use of bibliography. Receipt system will be used between Air Force and Contractor.

I. Reference Block 11c:

The contractor shall handle and protect classified materials. Any shipment of classified to or from the sites will be done through official government channels. The contractor is NOT authorized to transmit classified information to or from overseas locations.

J. Reference Block 11d:

The contractor must provide adequate storage for classified hardware to the level of SECRET, which exceeds two cubic feet.

K. Reference Block 11f:

The contractor will require access to classified information at Spangdahlem AB, Germany and Osan AB, Korea.

L. Reference Block 11h:

A COMSEC account will be established and COMSEC will be protected per National Security Agency (NSA) Industrial COMSEC Manual, NSA MAN 90-1.

M. Reference Block 11j:

See Requirement Document paragraph 2.2.3.4 for additional OPSEC requirements.

N. Reference Block 11i:

In accordance with DoD 5200.22M (NISPOM) chapter 5, section 4, paragraph 5-403f. The contractor shall be required to use Federal Express for overnight delivery of classified material when directed by the TSSC PO/QAR or the A-10 Program Office, OO-ALC/YWB. Classified shipments shall be prepared and shipped in accordance with guidance found in DoD 5200.22M (NISPOM) and DSS Industrial Security Letters (ISL).

O. Reference Block 14:

The contractor shall comply with the host base internal security program of the on-site facilities. The contractor shall secure the building upon leaving. The contractor shall comply with Air Force facility security plan. The contractor shall provide a point of contact for access to the facilities on-site during non-duty hours. All requests for non-duty access shall be coordinated through the PO or designated alternate. The contractor shall escort contract janitorial services and authorized personnel, performing building maintenance and upkeep. In case of an actual

emergency during non-duty hours, the PO or any other government personnel governed by local policy shall provide access to the on-site facilities for emergency personnel. Variations to this paragraph shall be made by a Long Term Visitor Group Security Agreement between the contractor and host base commander.

The contractor shall provide the information required by the Notification of Government Security Activity clause, AFFARS 5352.204-9000 and Visitor Group Agreements Clause, AFFARS, 5352.204-9001, to the Servicing Security Activity (SSA) addresses in block 17 of this form. Refer to contract document for these clauses.

P. Reference Block 15:

Contractor personnel, although recognized as employees and under administrative control of the contractor, shall be required to comply with the directives and requirements of the Wing Commander or authorized representative as to security regulations applicable to the described work site. Contractor personnel shall be subject to security investigations at all times and shall report any accident or incident with security implications to the PO and host base Security Forces.

Q. Reference Block 15:

Industrial security reviews while operating on an Air Force Installations will be conducted by the SSA.

R. Reference Block 17:

Required Distribution: one copy of DD Form 254 will be forwarded to the Chief of Security forces at the following locations,

355th SFS 3895 s. 6th street Davis Monthan AFB, Az 85707
43rd SFS Burgeon street Pope AFB, SC 28308
2nd SFS 425 Lindberg Street Barksdale AFB, LA 71110
62nd SFS/SFA 7 G street MT. Home AFB, ID 83648-5434
509th SFS/SFA 1031 Vandenberg Ave. Whiteman AFB, MO 65305
USAFE/SFI Unit 3220 Box 385, APO AE 09094-0384
103rd FW 100 Nicholson road Bradley ANGB, East Granby CT. 06026
110 FW Kellogg Airport 3545 mustang Ave. Battle Creek, MI. 49015
51st SFS/SFA Unit 2067 APO AP 96278-4044
52nd SFS/SFA Unit 3680 Box 220 APO AE 09126

S. Reference Block 17:

Required distribution at Hill AFB, UT

YWC_____

75 CS/SCBS_____

75 SFS/SFA _____

A. Reference Block 1:

Contractor personnel assigned to this program must be U.S. citizens with a minimum of a Secret Security Clearance based on current investigation. Contractor personnel will control access and protect classified information in accordance with the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22M. Contractor personnel must possess the required clearance prior to arrival on-site.

B. Reference Block 8a:

The work effort will be directed from TBD Company, and cage code 1DG67. In addition to the home office, contractor performance will also be conducted at the following sites: Davis Monthan AFB, AZ, Pope AFB, SC, Barksdale AFB, LA, New Orleans JRB, LA, Bradley ANGB, CT, Battle Creek ANGB, MI, Boise ANGB, ID, Whiteman AFB, MO, Osan AB, Korea, Spangdahlem AB, Germany, and the TSSC. The contractor is not authorized to transmit classified information to or from overseas locations.

C. Reference Block 8c:

The cognizant security office is the Chief of Security Forces at the actual location of contractor performance. Reference Blocks 8a and 17 for complete addresses.

D. Reference Block 10a:

COMSEC material /information may not be released to DoD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractors must forward requests for COMSEC material/information to the COMSEC officer through the program office. The contractor is governed by the DoD 5220.22s COMSEC supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances.

E. Reference Block 10a:

The Long Term Visitor Group Agreement between the Installation Commander and Contractor governs access to COMSEC material/information.

F. Reference Block 10g:

Any access to NATO classified information will require a final U.S. Government clearance at the appropriate level, and a NATO briefing.

G. Reference Block 10j:

FOUO information provided shall be safeguarded as specified in the attachment "Protecting for Official Use Only (FOUO) Information".

H. Reference Block 11c:

The contractor will require access to classified source data up to and including Secret in support of this effort. Any extracts or use of such data requires contractor to apply derivative classifications and markings consistent with the source documents. Use of "Multiple Sources" on the "Classified by" line necessitates compliance with the NISPOM, and use of bibliography. Receipt system will be used between Air Force and Contractor.

I. Reference Block 11c:

The contractor shall handle and protect classified materials. Any shipment of classified to or from the sites will be done through official government channels. The contractor is NOT authorized to transmit classified information to or from overseas locations.

J. Reference Block 11d:

The contractor must provide adequate storage for classified hardware to the level of SECRET, which exceeds two cubic feet.

K. Reference Block 11f:

The contractor will require access to classified information at Spangdahlem AB, Germany and Osan AB, Korea.

L. Reference Block 11h:

A COMSEC account will be established and COMSEC will be protected per National Security Agency (NSA) Industrial COMSEC Manual, NSA MAN 90-1.

M. Reference Block 11j:

See Requirement Document paragraph 2.2.3.4 for additional OPSEC requirements.

N. Reference Block 11i:

In accordance with DoD 5200.22M (NISPOM) chapter 5, section 4, paragraph 5-403f. The contractor shall be required to use Federal Express for overnight delivery of classified material when directed by the TSSC PO/QAR or the A-10 Program Office, OO-ALC/YWB. Classified shipments shall be prepared and shipped in accordance with guidance found in DoD 5200.22M (NISPOM) and DSS Industrial Security Letters (ISL).

O. Reference Block 14:

The contractor shall comply with the host base internal security program of the on-site facilities. The contractor shall secure the building upon leaving. The contractor shall comply with Air Force facility security plan. The contractor shall provide a point of contact for access to the facilities on-site during non-duty hours. All requests for non-duty access shall be coordinated through the PO or designated alternate. The contractor shall escort contract janitorial services and authorized personnel, performing building maintenance and upkeep. In case of an actual

emergency during non-duty hours, the PO or any other government personnel governed by local policy shall provide access to the on-site facilities for emergency personnel. Variations to this paragraph shall be made by a Long Term Visitor Group Security Agreement between the contractor and host base commander.

The contractor shall provide the information required by the Notification of Government Security Activity clause, AFFARS 5352.204-9000 and Visitor Group Agreements Clause, AFFARS, 5352.204-9001, to the Servicing Security Activity (SSA) addresses in block 17 of this form. Refer to contract document for these clauses.

P. Reference Block 15:

Contractor personnel, although recognized as employees and under administrative control of the contractor, shall be required to comply with the directives and requirements of the Wing Commander or authorized representative as to security regulations applicable to the described work site. Contractor personnel shall be subject to security investigations at all times and shall report any accident or incident with security implications to the PO and host base Security Forces.

Q. Reference Block 15:

Industrial security reviews while operating on an Air Force Installations will be conducted by the SSA.

R. Reference Block 17:

Required Distribution: one copy of DD Form 254 will be forwarded to the Chief of Security forces at the following locations,

355th SFS 3895 s. 6th street Davis Monthan AFB, Az 85707
43rd SFS Burgeon street Pope AFB, SC 28308
2nd SFS 425 Lindberg Street Barksdale AFB, LA 71110
62nd SFS/SFA 7 G street MT. Home AFB, ID 83648-5434
509th SFS/SFA 1031 Vandenberg Ave. Whiteman AFB, MO 65305
USAFE/SFI Unit 3220 Box 385, APO AE 09094-0384
103rd FW 100 Nicholson road Bradley ANGB, East Granby CT. 06026
110 FW Kellogg Airport 3545 mustang Ave. Battle Creek, MI. 49015
51st SFS/SFA Unit 2067 APO AP 96278-4044
52nd SFS/SFA Unit 3680 Box 220 APO AE 09126

S. Reference Block 17:

Required distribution at Hill AFB, UT

YWC _____

75 CS/SCBS _____

75 SFS/SFA _____

EMISSIONS SECURITY ASSESSMENT REQUEST (ESAR)
FOR ALL CLASSIFIED SYSTEMS

a. The contractor shall ensure that compromising emanations (EMSEC) conditions related to this contract are minimized.

b. The contractor shall provide countermeasures assessment data to the Contracting Officer (CO), in the form of an ESAR. The ESAR shall provide only specific responses to the data required in paragraph c, below. The contractor's standard security plan shall **NOT** be used as a "stand-alone" ESAR response. The contractor shall **NOT** submit a detailed facility analysis/assessment. The ESAR information will be used to complete an EMSEC Countermeasures Assessment Review of the contractor's facility to be performed by the government EMSEC authority using current Air Force EMSEC directives. EMSEC is applied on a case-by-case basis and further information may be required to complete the review. Should this be the case, the contractor shall provide this information to the contracting officer when requested. After the evaluation of the ESAR by the government EMSEC authority, additional EMSEC requirements **may** be established.

c. ESAR contents shall include, as a minimum, the following information (NISPOM, paragraph 11-101c) (Note: A copy of your Automated Information System Security Plan(s) (AISSP) will suffice.

(1) The specific classification and special categories of material to be processed or handled by electronic means.

(2) The percentage of information to be processed. Identify the approximate percentage for each level of information processed including unclassified.

(3) The specific location where classified processing will be performed.

(4) The name, address, title and telephone number of a point-of-contact at the facility where processing will occur.

NOTE: Once the above information has been provided to the CO, no further reporting is required for equipment reconfigurations. However, if the facility is physically relocated to another geographical location, the information requested in paragraph c above **MUST** be furnished to the CO.

d. The prime contractor shall ensure that all subcontractors and/or vendors comply with EMSEC requirements when performing classified processing related to this contract. They will provide the above documentation through their prime to the contracting officer to complete the ESAR.

FOR OFFICIAL USE ONLY (FOUO)
(DOD REGULATION 5400.7-R, AIR FORCE SUPPLEMENT)
REF. TO ITEM 10J OF DD FORM 254

FOUO is not a classification. Originators mark records when they create them to call attention to FOUO content. An FOUO marking does not mean you must withhold a record under the FOIA. You still need to review requested records. Examine records with and without markings to identify information that needs protection and is exempt from public release or to decide whether discretionary release is appropriate.

Information in a technical document that requires a distribution statement per AFI 61-204, Disseminating Scientific and Technical Information, must show that statement. The originator may also mark the information FOUO, if appropriate.

Mark an unclassified document containing FOUO information "For Official Use Only" at the bottom, on the outside of the front cover (if any), on each page containing FOUO information, on the back page, and on the outside of the back cover (if any).

In unclassified documents, the originator may also mark individual paragraphs that contain FOUO information to alert users and assist in review.

In a classified document, mark: An individual paragraph that contains FOUO, but not classified information, by placing "(FOUO)" at the beginning of the paragraph.

The top and bottom of each page that has both FOUO and classified information, with the highest security classification of information on that page.

"FOUO" at the bottom of each page that has FOUO but not classified information.

If a classified document also contains FOUO information or if the classified material becomes FOUO when declassified, place the following statement on the bottom of the cover or the first page, under the classification marking: NOTE: If declassified, review the document to make sure material is not FOUO and not exempt under DoD 5400.7, AF Supplement before public release.

Mark other records, such as computer printouts, photographs, films, tapes, or slides, "For Official Use Only" or "FOUO" so the receiver or viewer knows the record contains FOUO information.

Mark FOUO material sent to authorized persons outside the DoD with an explanation typed or stamped on the document.

Transmitting FOUO:

DoD components, officials of DoD components, and authorized DoD contractors consultants, and grantees send FOUO information to each other to conduct official DoD business. Tell

recipients the status of such information, and send the material in a way that prevents unauthorized public disclosure. Make sure documents that transmit FOUO material call attention to any FOUO attachments. Normally, you may send FOUO records over facsimile equipment. When deciding whether to send FOUO records over facsimile equipment, balance the sensitivity of the records against the risk of disclosure. To prevent unauthorized disclosure, consider attaching special cover sheets (i.e. AF Form 3227, Privacy Act Cover Sheet, for Privacy Act Information), the location of sending and receiving machines, and ensure authorized personnel are available to receive FOUO information as soon as it is transmitted. FOUO information may be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Mark the records "For Official Use Only," and tell the recipient the information is exempt from public disclosure under the FOIA and whether it needs special handling.

Electronically and Facsimile Transmitted Messages. Each part of electronically and facsimile transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text. Such messages and facsimiles shall be transmitted in accordance with communications security procedures whenever practicable.*

Transporting FOUO:

Records containing FOUO information shall be transported in a manner that prevents disclosure of the contents. When not commingled with classified information, FOUO information may be sent via first-class mail or parcel post. Bulky shipments, such as distributions of FOUO Directives to testing materials, that otherwise qualify under postal regulations may be sent by fourth class mail.

Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

Safeguarding FOUO Information:

During normal duty hours: During normal working hours, records determined to be FOUO shall be placed in an out-of-sight location if the work area is accessible to non-government personnel.

During Nonduty Hours: At the close of business, FOUO records shall be stored so as to prevent unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during nonduty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. FOUO records that are subject to the provisions of the National Security Act of 1959 (reference (aa)) shall meet the safeguards outlined for that group of records.

Termination, Disposal and Unauthorized Disclosures:

Termination: The originator or other competent authority; e.g., initial denial and appellate authorities, shall terminate "For Official Use Only" markings or status when circumstances indicate that the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the "For Official Use only" markings, but records in file or storage need not be retrieved solely for that purpose.

Disposal: Nonrecord copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing, and placing them in regular trash containers. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

Record copies of FOUO documents shall be disposed of in accordance with the disposal standards established under 44 U.S.C. 3301-3314 (reference (ab)), as implemented by DoD Component instructions concerning records disposal.

Unauthorized disclosure: The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act (reference (d)) may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

***NOTE:** For clarification of electronic dissemination, FOUO will not be sent electronically unless it remains behind the Hill AFB/SINET Firewall.

~~SECRET~~
31-209

OPERATIONS SECURITY (OPSEC)
ANNEX 1 TO HAFB PLAN 31-101
Addendum to DD Form 254, Item 11.j.

GENERAL:

1. **PURPOSE:** This section outlines the requirements and procedures necessary to protect Critical Information for Operations Security (OPSEC).
2. **MISSION:** To maintain a continuing awareness of adversary interest in this centers actions and adversary intelligence collection capabilities. To understand the need to identify and protect classified and unclassified indicators which occur reveal sensitive information. To evaluate the effectiveness of OPSEC measures taken to preclude or reduce adversary acquisition and exploitation of sensitive information.
3. **DEFINITION:** OPSEC is the process of analyzing friendly actions attendant to military operations and other activities to:

- a. Identify those actions that can be observed by adversary intelligence systems.
- b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- c. Select and execute measure that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

4. **OBJECTIVES:**

- a. To protect planned mobilization activities by preventing the inadvertent disclosure of unclassified information relating to or revealing a possible classified operation.
- b. To preserve secrecy concerning specific scenario events an US response to these events.
- c. To identify OPSEC vulnerabilities and recommend protective measure which will serve to enhance the security of future contingency operations.

5. **TASKS:**

- a. All OO-ALC directorates and Staff organizations OPSEC Officers will give an initial OPSEC briefing to all personnel assigned to their organizations.
- b. The organizations OPSEC point-of-contact will make sure that each Individual Mobilization Augmentee (IMA) is familiar with his/her units Critical Information. The initial OPSEC briefing to an IMA will be documented on the military member's record.